

"Express Mail" Mailing Label No. EL436467612US

PATENT APPLICATION
ATTORNEY DOCKET NO. NA00-02401

5

10

**METHOD AND APPARATUS FOR
CONTENT-BASED INTRUSION DETECTION
USING AN AGILE KERNEL-BASED AUDITOR**

15

Inventor: Cheuk W. Ko

GOVERNMENT LICENSE RIGHTS

20

This invention was made with United States Government support under contract #F30602-96-C-0333 funded by the Defense Advanced Research Projects Agency (DARPA) through Rome Labs. The United States Government has certain rights in the invention.

25

BACKGROUND

Field of the Invention

The present invention relates computer security and intrusion detection systems. More specifically, the present invention relates to a method and an

apparatus for providing content-based intrusion detection using an agile kernel-based auditor.

Related Art

5 As computers become increasingly more interconnected, it is becoming progressively harder to safeguard computer systems from attacks launched across computer networks. Several types of attacks, such as buffer overflow attacks, and attacks that make unauthorized modifications to data objects, can be detected by examining data that is being read to and/or written from security critical files or
10 network connections.

 Unfortunately, existing intrusion detection systems cannot reliably detect these types of attacks because they do not possess the ability to examine data that is being read or written during system calls.

 For example, an existing auditing system may record system call
15 parameters or attributes of subjects and objects involved in the system calls. However, existing auditing systems do not record data that is being read from or written to files or network connections because the volume of data that is read or written is prohibitively large.

 Some network sniffers can collect data being read from and/or written to
20 files across a network. However, network sniffers cannot gather information regarding accesses to local files. Furthermore, network sniffers can suffer performance and packet-loss problems if they try to collect this type of data because as mentioned previously the volume is prohibitively large. Also, encryption is increasingly being used to protect the privacy of data transmitted
25 across networks. Consequently, network sniffers will eventually be unable to obtain useful audit data.

005330.061300

Hence, what is needed is a method and apparatus for monitoring systems calls that gathers read and/or write data for intrusion detection purposes without encountering problems in handling large volumes of data.

5 Another problem is that existing auditing systems are not configured to collect information for specific intrusion detection systems. Existing auditing systems are typically developed by operating system developers, who do not necessarily know what types of data are required by intrusion detection systems. Consequently, existing auditing systems are not configured to gather parameters and/or other attributes that are required by an intrusion detection system.

10 Furthermore, an intrusion detection system may require different types of data to be gathered at different times.

Hence, what is needed is a method and an apparatus that can be configured to selectively gather specific system call information for an intrusion detection system.

15

SUMMARY

One embodiment of the present invention provides content-based intrusion detection for a computer system by using an agile kernel-based auditing system. This auditing system operates by receiving an audit specification that specifies target attributes to be recorded during an auditing process. The audit specification

20 also specifies an auditing criterion that triggers recording of the target attributes. Upon receiving the audit specification, the auditing system is configured to record the target attributes during system calls whenever the auditing criterion is satisfied. Next, an application program is monitored by the auditing system to produce an audit log containing the recorded target attributes. This audit log is

25 examined in order to detect patterns for intrusion detection purposes.

09593280 "061300

In one embodiment of the present invention, configuring the auditing system involves compiling the audit specification to produce a kernel module, and then loading the kernel module into a kernel of an operating system. It also involves linking code from within the kernel module into system calls within the operating system.

In one embodiment of the present invention, in response to detecting an event during the auditing process, the system dynamically adjusts the auditing system to change the auditing criterion and/or the target attributes for subsequent operation of the auditing system.

In one embodiment of the present invention, the auditing system is configured to modify a system call jump table to cause selected system calls to execute code that causes the target attributes to be recorded in response to the auditing criterion being satisfied.

In one embodiment of the present invention, the target attributes can include: an argument from a system call; a parameter of a process making the system call; data read during the system call; data written during the system call; a parameter of a file involved in the system call; and a parameter relating to a network communication involved in the system call.

In one embodiment of the present invention, the auditing criterion can include: a user identifier for a process that is making a system call; an identifier for an application program from which the system call is being made; and an identifier for a file being accessed by the system call.

In one embodiment of the present invention, producing the audit log involves filtering the target attributes to reduce an amount of data stored in the audit log.

ID, a group ID, an effective group ID, a parent process ID, a session ID and a pathname for the process), data read during the system call, data written during the system call, a parameter related to a file involved in the system call (such as a permission mode, an inode number, a device ID, a time of creation, an owner user
5 ID and a file type) or a parameter related to a network communication involved in the system call (such as an IP address or port number).

Also note that the auditing criterion can generally include any specifier for a condition associated with a system call, including a user identifier for a process that is making the system call, an identifier for an application program from which
10 the system call is being made or an identifier for a file being accessed by the system call. Note that the condition is satisfied if a currently used identifier matches the specified identifier. For example, if the identifier specifies a password file, if the password file is being currently accessed, the condition is satisfied.

15 Next code 306 calls the real underlying system call through real system call interface 114.

After the real system call returns, code 306 can record another target attribute in response to detecting another auditing criterion. This capability is useful for recording the result of the real system call.

20

Process of Configuring and Running Auditing System

FIG. 4 is a flow chart illustrating the process of configuring and running the auditing system in accordance with an embodiment of the present invention. The system starts by receiving audit specification 202 (step 402). In one
25 embodiment of the present invention, audit specification 202 is received from either a human user of the auditing system, or from an intrusion detection mechanism that automatically generates audit specification 202.

